were rejected under 35 U.S.C. §103(a) as unpatentable over Adams, Jr. et al; Claims 12 and 13 were rejected under 35 U.S.C. §103(a) as unpatentable over Adams, Jr. et al in view of Perlman; and Claims 17 and 18 were rejected under 35 U.S.C. §103(a) as unpatentable over Adams, Jr. et al in view of Saito.

Regarding the objection to Claims 11, 17 and 19, Claims 17 and 19 have been amended in light of the comments noted in the outstanding Office Action and as shown in the marked-up copies. Further, regarding Claim 11, the outstanding Office Action indicates the second "and" term in line 25 is improperly located. However, Applicants respectfully note this "and" term is properly located (i.e., the relay device comprises a first interface, a second interface, a first contents protection unit, a second contents protection unit, a contents reception unit AND a contents transmission unit). Accordingly, it is respectfully requested this objection be withdrawn.

Regarding the rejection of Claims 1, 2, 5 and 17-19 under 35 U.S.C. §112, second paragraph, the appropriate claims have been amended in light of the comments noted in the outstanding Office Action and as shown in the marked-up copies. Further, regarding Claims 1, 2 and 5, the outstanding Office Action indicates that the term "control command signal" is a relative term which renders the claim indefinite and the specification does not provide a standard for ascertaining the requisite degree. Applicants note the term "control command signals" refers to the AV/C signals discussed in the specification (i.e., the signals corresponding to the control command signals refer to the radio node control packet discussed in the specification). Accordingly, it is respectfully requested this rejection be withdrawn.

Claims 1, 5-11, 14-16 and 19 stand rejected under 35 U.S.C. §102(b) as anticipated by Adams, Jr. et al. This rejection is respectfully traversed.

The present invention currently includes independent Claims 1, 2, 5, 11-14 and 16-19. Independent Claims 1, 5, 11, 14, 16 and 19 will be discussed regarding this rejection and independent Claims 2, 12, 13 and 17 will be discussed later.

Regarding independent Claim 1, the outstanding Office Action interprets the claimed proxy unit as acting transparent to a different network. However, the claimed proxy configuration unit is not acting transparent to a different network because the proxy unit is required to disclose a device/service/sub-unit on a second network as if it is a device/service/sub-unit provided by the relay device to the first network. This means that what is actually on the second network is seen as being on the relay device from the viewpoint of the first network. Therefore, the relay device is not transparent from the first network (i.e., the first network can "see" the relay device). Further, the claimed proxy configuration unit ensures that a device/service/sub-unit on the second network is made to appear as if it is provided by the relay device from the viewpoint of the first network, because the first network cannot recognize a device/service/sub-unit on the second network when the first and second networks are operated by different protocols.

Regarding the cited portion of Adams, Jr. et al (column 4, lines 37-39) as teaching the claimed proxy unit, Applicants note this section is silent about a proxy unit able to ensure that a device on a second network is viewed as being on the first network, as discussed above.

The outstanding Office Action also indicates Adams, Jr. et al disclose the claimed control command reception and transmission units and cites column 1, lines 47-58 and column 5, lines 12-20. The claimed control command reception and transmission units are required to receive the control command signals (such as AV/C) from the first network side and transmit the signals to the second network side.

On the contrary, column 1, lines 47-58 of Adams, Jr. et al only describe exchanging control information and data between different layers at one and the same node, and not from one network to another network as claimed. Further, column 5, lines 12-20 only describe the connection relationship of the microprocessor 20 with the other components within one and the same device (CNEDD), and does not describe transferring the control command signals from one network to another network via the relay device.

The outstanding Office Action also indicates Adams, Jr. et al teach the claimed contents protection information reception and transfer units and cites column 6, lines 21-29 and column 4, lines 40-52.

The claimed contents protection information reception and transfer units are required to receive the contents protection information from the first network side and transfer the information to the second network side without making any changes. Thus, the claimed relay device is transparent in this regard because the contents protection information is transferred from the first network side to the second network side as if the relay device does not exist therebetween.

However, column 6, lines 21-29 of Adams, Jr. et al only describe the second and third elements in the key list structure used by the microprocessor 20 of the CNEDD 10 to decide whether the received data packet should be encrypted, decrypted, passed through or deleted. Adams, Jr., et al do not teach or suggest transferring the contents protection information from one network to another network via the relay device. Further, column 4, lines 40-52 only describe a table used for the purpose of routing or the encryption/decryption decision.

Similar arguments apply to independent Claim 5 with respect to the claimed proxy configuration unit and the claimed control command reception and transmission units.

Independent Claim 5 also includes additional features including first and second contents protection units and contents reception and transfer units. Regarding these features, the outstanding Office Action indicates Adams, Jr. et al teach the claimed first and second contents protection units and cites column 6, lines 6-16 and 21-29 and column 6, line 65 to column 7, line 1.

The claimed first and second contents protection units are required to perform the contents protection procedure separately with respect to a device/service/sub-unit on the first network side and with respect to a device/service/sub-unit on the second network side.

However, column 6, lines 6-16 of Adams, Jr. et al only describe the encryption of the IP data packet received from the downstream network. Further, column 6, lines 21-29 only describe the second and third elements in the key list structure used by the microprocessor 20 of the CNEDD 10 to decide whether the received data packet should be encrypted, decrypted, passed through or deleted. This section does not teach or suggest the separate contents protection procedures for the first and second networks. In addition, column 6, line 65 to column 7, line 11 only describe a reconstruction of an IP data packet.

The outstanding Office Action also indicates Adams, Jr. et al teach the claimed contents reception and transfer units and cites column 6, lines 6-16 and 21-29 and column 6, line 65 to column 7, line 11. However, as discussed above, these sections merely relate to the encryption of the IP data packet, and the description of the second and third elements in the key list and reconstruction of an IP data packet.

Similar arguments apply to independent Claim 11 with regard to the first and second contents protection units and the contents reception and transfer units as discussed above with respect to independent Claim 5. Independent Claim 11 also includes a wherein clause in which a first key information used in the contents protection procedure in the first contents

protection unit and a second key information used in the contents protection procedure in the second contents protection unit are set to be identical. The outstanding Office Action indicates Adams et al teach this feature and cites column 6, line 65 to column 7, line 11 and column 5, line 65 to column 6, line 5. However, column 6, line 65 to column 7, line 11 only describe the reconstruction of an IP data packet. Further, column 5, line 65 to column 6, line 5 only describe that each IP data packet consists of data characters, header characters and trailer characters.

Regarding independent Claim 14, the outstanding Office Action indicates Adams et al teach the claimed contents transfer unit and cites column 4, lines 40-44, column 5, line 66 to column 6, line 5 and column 6, lines 17-20.

The claimed contents transfer unit is required to transmit or receive the encrypted contents through a flow identified by a set of a source address, a source port, a destination address and a destination port. On the contrary, column 4, lines 40-44 of Adams, Jr. et al only describe a table used for the purpose of routing or the encryption/decryption decision. Further, as noted above, column 5, line 65 to column 6, line 5 only describe that the each IP data packet consists of data characters, header characters, and trailer characters. Column, lines 17-20 only describe the three separate elements constituting the key list structure.

The outstanding Office Action also indicates Adams, Jr. et al teach the claimed copy protection processing unit and cites column 4, lines 40-52 and column 6, lines 21-20.

The claimed copy protection processing unit is required to carry out the contents protection procedure including the authentication procedure and/or the key exchange procedure in units of the flow. On the contrary, column 4, lines 40-52 of Adams, Jr. et al only describe a table used for the purpose of routing or the encryption/description decision. Column 6, lines 21-29 only describe the second and third elements in the key list structure

used by the microprocessor 20 of the CNEDD 10 to decide whether the received data packet should be encrypted, decrypted, passed through or deleted. Further, Adams, Jr. et al do not teach or suggest transferring the contents from one network to another network via the relay device.

The outstanding Office Action also states the claimed contents protection procedure is encryption. However, Applicants note it is well known a contents protection procedure such as the authentication procedure and the key exchange procedure is totally different from encryption.

Similar arguments apply to independent Claim 16 with respect to the claimed copy protection processing unit discussed in Claim 14 and the contents transmission and reception unit with respect to Claim 5. Further, Claim 16 also includes a wherein clause which recites that at least one of an identifier of a service, a sub-unit, a virtual channel, or a plug that carries out exchange of the encrypted contents, and an identifier by which the encrypted contents can be uniquely identified by a transmitting side device, is attached to information exchanged in at least a part of procedures included in the contents protection procedure.

The outstanding Office Action indicates Adams, Jr. et al teach this feature and cites column 5, line 61 to column 6, line 5. However, as discussed above, this section only describes that each IP data packet consists of data characters, header characters and trailer characters.

Similar arguments apply to independent Claim 19 for the claimed first and second contents protection units and the contents reception and transmission units as that discussed above with respect to Claim 5. Claim 19 also includes a wherein clause in which the outstanding Office Action states is disclosed in column 5, line 61 to column 6, line 11 of

Adams Jr, et al. However, as noted above, this section only describes that each IP data packet consists of data characters, header characters, and trailer characters.

Accordingly, it is respectfully submitted independent Claims 1, 5, 11, 14, 16 and 19 and each of the claims depending therefrom patentably define over Adams, Jr. et al.

Claims 2-4 stand rejected under 35 U.S.C. §103 as unpatentable over Adams, Jr. et al. This rejection is respectfully traversed.

Similar arguments apply to the claimed proxy configuration unit, control command reception and transmission units and contents protection information reception and transfer units as that discussed above with respect to Claim 1.

Further, the outstanding Office Action recognizes that Adams, Jr. et al fail to teach or suggest the claimed contents reception and transfer units, but indicates that these features are obvious. However, the claimed contents reception and transfer units are required to receive the contents from the one network side and transfer the contents to the other network side without making any changes. Thus, as discussed above, the claimed relay device is transparent in this regard because the contents are transferred from the one network side to the other network side as if the relay device does not exist therebetween. Adams, Jr. et al do not teach or suggest transferring the contents transparently from one network to another network via the relay device.

Claims 12 and 13 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Adams, Jr et al in view of Perlman. This rejection is respectfully traversed.

Regarding independent Claim 12, the outstanding Office Action indicates Adams, Jr. et al teach the claimed copy protection processing unit and cites column 4, lines 40-52.

The claimed copy protection processing unit is required to carry out the contents protection procedure including the authentication procedure and/or the key exchange

procedure. However, as noted above, column 4, lines 40-52 of Adams, Jr. et al only describe a table used for the purpose of routing or the encryption/decryption decision.

The outstanding Office Action also interprets the claimed key exchange procedure as a mechanism to maintain lists of keys for sites so as to change keys for respective sites. However, the key exchange procedure is well-known to be a procedure for exchanging keys for the purpose of sharing the keys at both sides.

The outstanding Office Action also indicates Adams, Jr. et al teach the claimed contents transmission unit and cites columns 6, lines 17-29 and column 6, line 65 to column 7, line 1. The claimed contents transmission is required to transmit the encrypted contents either to a virtual channel on the network or by further attaching identifier by which encrypted contents can be uniquely identified by the communication device.

On the contrary, column 6, lines 17-20 in Adams, Jr. et al only describe the three separate elements constituting the key list structure. Further, as noted above, column 6, lines 21-29 only describe the second and third elements in a key list structure used by the microprocessor 20 of the CNEDD 10 to decide whether the received data packet should be encrypted, decrypted, passed through, or deleted. As noted above, Adams, Jr. et al do not teach or suggest transferring the contents from one network to another network via the relay device and column 6, line 65 to column 7, line 11 only describe the reconstruction of an IP data packet.

The outstanding Office Action also recognizes that Adams, Jr. et al fail to teach or suggest the claimed reception unit and the claimed notification unit, and indicates these features are shown in Perlman and cites column 14, lines 38-39.

The claimed reception unit is required to receive a query regarding a service/sub-unit/plug that is transferring the encrypted contents, and the claimed notification unit is

required to notify a service/sub-unit/plug that is transferring the encrypted contents in response to the query.

However, column 14, lines 38-49 of Perlman only describe a network manager which queries each node to determine if it received a particular packet and each node responds to the query. The query and response are not a query and encrypted contents.

Regarding independent Claim 13, the outstanding Office Action indicates Adams, Jr. et al teach the claimed copy protection unit. However, as noted above with respect to Claim 12, Adams, Jr. et al do not teach or suggest the claimed copy protection processing unit. Similar arguments apply to the claimed contents reception unit.

The outstanding Office Action also indicates Adam, Jr. et al do not teach or suggest the claimed transmission and reception units and relies on Perlman as disclosing these features and cites column 14, lines 38-49. However, as noted above with regard to Claim 12, column 14, lines 38-49 of Perlman only describe the network manager which queries each node to determine if it received a particular packet and each node responds to the query.

Accordingly, it is respectfully submitted independent Claims 2, 12 and 13 and each of the claims depending therefrom are also allowable.

Claims 17 and 18 stand rejected under 35 U.S.C. §103(a) as unpatentable over Adams, Jr. et al in view of Saito. This rejection is respectfully traversed.

Regarding independent Claim 17, the outstanding Office Action indicates Adams, Jr. et al teach the claimed first and second claimed copy protection units and cites column 4, lines 40-52. Again, however, as noted above, column 4, lines 40-52 of Adams, Jr. et al only describe a table used for the purpose of routing or the encryption/decryption decision.

The outstanding Office Action also indicates the claimed key exchange procedure is a mechanism to maintain a list of keys for sites so as to change a key for respective sites.

However, as noted above, the key exchange procedure is well-known to be a procedure for exchanging keys for the purpose of sharing the keys at both sides.

The outstanding Office Action also indicates Adam, Jr. et al teach the claimed contents reception unit, the claimed decryption unit, the claimed encryption unit, and the claimed contents transmission unit and cites column 6, lines 6-16 and 21-29, column 6, line 65 to column 7, line 11 and column 7, lines 19-33.

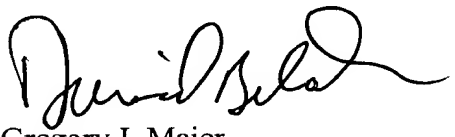
However, as noted above, column 6, lines 6-16 only describe the encryption of the IP data packet received from the downstream network, and column 6, lines 21-29 only describe the second and third elements in the key list structure used by the microprocessor 20 of the CNEDD 10 to decide whether the received data packet should be encrypted, decrypted, passed through, or deleted. Further, column 6, line 65 to column 7, line 11 only describes a reconstruction of an IP data packet. In addition, column 7, lines 19-33 only describe the decryption of the received data packet.

Accordingly, it is respectfully requested this rejection also be withdrawn.

Consequently, in light of the above discussion and in view of the present amendment, the present application is believed to be in condition for allowance and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier
Attorney of Record
Registration No. 25,599
David A. Bilodeau
Registration No. 42,325

22850

(703) 413-3000
Fax #: (703)413-2220
DAB/smi

I:\atty\DAB\00397378-am.wpd

Marked-Up Copy
Serial No: 09/404,547
Amendment Filed on:
January 31, 2003

IN THE CLAIMS

Please amend Claims 2, 6, 17 and 19 as follows:

--2. (Amended) A relay device, comprising:

a first interface unit connected to a first network;

a second interface unit connected to a second network;

a proxy configuration unit for disclosing each device/service/sub-unit on the first network or the second network as an own device/service/sub-unit provided on the relay device with respect to respective another network side;

a control command reception unit for receiving control command signals destined to the own device/service/sub-unit from a side of one network to which the own device/service/sub-unit is disclosed by the proxy configuration unit;

a control command transmission unit for transmitting signals corresponding to the control command signals received by the control command reception unit, to [said] each device/service/sub-unit on another network different from said one network;

a contents protection information reception unit for receiving contents protection information destined to the own device/service/sub-unit from a device on the first network or the second network;

a contents protection information transfer unit for transferring the contents protection information received by the contents protection information reception unit to said each

device/service/sub-unit on said another network, without making any change in the contents protection information;

a contents reception unit for receiving contents destined to the own device/service/sub-unit and protected by a contents key obtained from the contents protection information, from a device on the first network or the second network; and

a contents transfer unit for transferring the contents received by the contents reception unit to said each device/service/sub-unit on said another network, without making any change in the contents.

6. (Amended) The relay device of claim 5, wherein the first contents protection unit and the second contents protection unit use different encryption schemes or identical encryption [scheme] schemes based on different [key information] keys.

17. (Amended) A relay device, comprising:

a first interface unit connected to a first network;

a second interface unit connected to a second network;

a first copy protection processing unit for carrying out a prescribed contents protection procedure including at least an authentication procedure and a key exchange procedure, with respect to one device/service/sub-unit on the first network;

a second copy protection processing unit for carrying out the prescribed contents protection procedure including at least an authentication procedure and a key exchange procedure, with respect to another device/service/sub-unit on the second network;

a contents reception unit for receiving encrypted data containing [specific] contents from the first interface unit;

a decryption unit for decrypting the encrypted data [receiving] received by the contents reception unit, by using a contents protection key provided by the first copy protection processing unit, to obtain decrypted data;

a conversion unit for converting the decrypted data into converted data in another coding format;

an encryption unit for encrypting the converted data, by using a contents protection key provided by the second copy protection processing unit, to obtain re-encrypted data; and

a contents transmission unit for transferring the re-encrypted data to the second interface unit.

19. (Amended) A relay device, comprising:

a first interface unit connected to a first network;

a second interface unit connected to a second network;

a first contents protection unit for carrying out a contents protection procedure with respect to one device/service/sub-unit on the first network;

a second contents protection unit for carrying out the contents protection procedure with respect to another device/service/sub-unit on the second network;

a contents reception unit for receiving contents destined to an own device/service/sub-unit on the relay device and encrypted according to one of the first and second contents protection units, from a device on one of the first network and the second networks; and

a contents transmission unit for [transmittting] transmitting the contents received by the contents reception unit to a device/service/sub-unit on another one of the [frist] first network and the second network, by encrypting the contents according to another one of the first and second contents protection units;

wherein said one of the first and second contents protection units carries out an authentication and/or a key exchange with a device/service/sub-unit on said one of the first network and the second network by referring to [a relationship between] states of the contents reception unit and the contents transmission unit, when there is a request for a [precedure] procedure of the authentication and/or the key exchange with respect to said another one of the first and second contents protection units.--